CUNOAȘTEREA ȘTIINȚIFICĂ

ISSN 2821 – 8086, ISSN – L 2821 – 8086, Volumul 3, Numărul 2, Iunie 2024

Provocări și tendințe în războiul electronic – Războiul asimetric

Nicolae SFETCU

Sfetcu, Nicolae (2024), Provocări și tendințe în războiul electronic – Războiul asimetric, *Cunoașterea Științifică*, **3**:2, 49-55, DOI: 10.58679/cs25350, https://www.cunoasterea.ro/provocari-si-tendinte-in-razboiul-electronic-razboiul-asimetric/

Publicat online: 15.02.2024

© 2024 Nicolae SFETCU. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

Provocări și tendințe în războiul electronic – Războiul asimetric

Ing. fiz. Nicolae SFETCU[1], MPhil
nicolae@sfetcu.com

Challenges and Trends in Electronic Warfare – Asymmetric Warfare

Abstract

Electronic warfare was conceived a quarter of a century ago, developing through the exponential growth of space and cyber technologies that rely primarily on electromagnetic signals. But the electromagnetic environment (EME) is an operational environment that must be configured to support electromagnetic operations (EMO). The modern challenges of dealing with advanced adversary capabilities, particularly in confrontations requiring access and area denial operations, have brought electromagnetic warfare (EW) back to the fore. NATO is currently rewriting its EW doctrine and investigating how to operate more effectively in the electromagnetic spectrum (EMS). This essay explores the distinctive features of asymmetric warfare and analyzes the challenges and emerging trends in electronic warfare in this context.
Keywords: electronic warfare, electromagnetic warfare, asymmetric warfare, cognitive electronic warfare, distributed electronic warfare

Rezumat

Războiul electronic a fost conceput în urmă cu un sfert de secol, dezvoltându-se prin creșterea exponențială a spațiului și a tehnologiilor cibernetice care se bazează, în primul rând, pe semnale electromagnetice. Dar mediul electromagnetic (EME) este un mediu operațional care trebuie configurat pentru a sprijini operațiunile electromagnetice (EMO). Provocările moderne de a face față capacităților de vârf ale adversarilor, în special în confruntările care necesită operațiuni de acces și refuzare zonală, au readus războiul electromagnetic (EW) în prim plan. În prezent, NATO își rescrie doctrina EW și investighează cum să opereze mai eficient în spectrul electromagnetic (EMS). Acest eseu explorează caracteristicile distinctive ale războiului asimetric și analizează provocările și tendințele emergente în războiul electronic în acest context.
Cuvinte cheie: războiul electronic, războiul electromagnetic, războiul asimetric, războiul electronic cognitiv, războiul electronic distribuit

[1] Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

CUNOAȘTEREA ȘTIINȚIFICĂ, Volumul 3, Numărul 2, Iunie 2024, pp. 49-55
ISSN 2821 – 8086, ISSN – L 2821 – 8086, DOI: 10.58679/cs25350
URL: https://www.cunoasterea.ro/provocari-si-tendinte-in-razboiul-electronic-razboiul-asimetric/
© 2024 Nicolae SFETCU. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

Acesta este un articol cu Acces Deschis (Open Access) distribuit în conformitate cu termenii licenței de atribuire Creative Commons CC BY SA 4.0 (https://creativecommons.org/licenses/by-sa/4.0/).

Introducere

Războiul electronic a fost conceput în urmă cu un sfert de secol, dezvoltându-se prin creșterea exponențială a spațiului și a tehnologiilor cibernetice care se bazează, în primul rând, pe semnale electromagnetice. Dar mediul electromagnetic (EME) este un mediu operațional care trebuie configurat pentru a sprijini operațiunile electromagnetice (EMO). Provocările moderne de a face față capacităților de vârf ale adversarilor, în special în confruntările care necesită operațiuni de acces și refuzare zonală, au readus războiul electromagnetic (EW) în prim plan. În prezent, NATO își rescrie doctrina EW și investighează cum să opereze mai eficient în spectrul electromagnetic (EMS).

Războiul electronic (EW) a devenit un domeniu critic în războiul modern, în special în contextul conflictelor asimetrice în care armatele avansate din punct de vedere tehnologic se confruntă cu adversari neconvenționali. Războiul asimetric prezintă provocări și tendințe unice în războiul electronic, solicitând strategii și tehnologii inovatoare pentru a menține superioritatea.

Înțelegerea războiului asimetric

Războiul asimetric se referă la conflicte între adversari inegali, în care o parte are capacități militare semnificativ superioare în comparație cu cealaltă. În astfel de scenarii, partea mai slabă

recurge adesea la tactici neconvenționale, inclusiv război de gherilă, terorism și atacuri cibernetice, pentru a neutraliza avantajele adversarului mai puternic. Spre deosebire de războiul convențional, conflictele asimetrice se caracterizează prin complexitatea, ambiguitatea și imprevizibilitatea lor, punând provocări distincte pentru planificatorii și operatorii militari.

Războiul electronic joacă un rol crucial în scenariile contemporane de război asimetric, în care armatele avansate din punct de vedere tehnologic se angajează cu actori nestatali sau cu adversari mai puțin avansați.

Războiul asimetric, caracterizat prin disparități în capacitățile militare între forțele opuse, a devenit o trăsătură definitorie a conflictului contemporan. În astfel de situații, utilizarea tehnologiei avansate, în special în domeniul războiului electronic, are un impact profund asupra rezultatului conflictelor. EW cuprinde o gamă largă de activități care implică utilizarea spectrului electromagnetic pentru a exploata, proteja și controla sistemele de informații și comunicații.

Războiul electronic are un impact profund asupra tacticilor și strategiilor folosite în războiul asimetric. Pentru militarii avansați, oferă un avantaj asimetric, permițându-le să neutralizeze limitările tehnologice ale adversarilor lor. Ei pot opera în medii ostile cu o conștientizare îmbunătățită a situației, pot efectua lovituri precise și pot minimiza daunele colaterale. Cu toate acestea, actorii nestatali și adversarii mai puțin avansați s-au adaptat și ei la provocărilor generate de războiul electronic. Ei au recurs la metode de comunicare nestandardizate, cu tehnologie scăzută, și au căutat refugiu în zone în care războiul electronic poate avea o eficiență limitată.

Conflictele în curs din Orientul Mijlociu oferă exemple notabile de război electronic în războiul asimetric. Armatele avansate, cum ar fi Statele Unite și aliații săi, au folosit războiul electronic pentru a perturba rețelele de comunicații ale grupurilor insurgente și pentru a localiza

ținte de mare valoare. Pe de altă parte, actori nestatali, cum ar fi Statul Islamic, s-au adaptat utilizând canale de comunicare criptate și tactici low-tech pentru a evita supravegherea și atacul electronic.

Provocări în războiul electronic

Războiul electronic în războiul asimetric întâmpină mai multe provocări care decurg din natura conflictului:

- *Tactici adaptive*: adversarii asimetrici își adaptează constant tacticile și strategiile pentru a exploata vulnerabilitățile din sistemele electronice ale adversarului. Ei folosesc abordări agile și dinamice pentru a evita detectarea, a întrerupe comunicațiile și a înșela senzorii, ceea ce face dificil pentru forțele superioare din punct de vedere tehnologic să anticipeze și să contracareze acțiunile lor.
- *Reguli limitate de angajare*: conflictele asimetrice apar adesea în medii cu reguli ambigue de angajare și granițe neclare între combatanți și necombatanți. Acest lucru complică utilizarea tehnicilor de război electronic, deoarece forțele militare trebuie să navigheze pe considerente juridice și etice în timp ce se angajează cu adversari care ar putea să nu adere la normele tradiționale de război.
- *Constrângeri de resurse*: Spre deosebire de armatele convenționale cu resurse substanțiale dedicate războiului electronic, adversarii asimetrici operează cu bugete limitate și acces la tehnologie avansată. Cu toate acestea, ei compensează aceste limitări prin inovație și creativitate, valorificând echipamente ieftine comerciale de la raft (COTS) și tehnici improvizate pentru a-și atinge obiectivele.
- *Managementul spectrului*: spectrul electromagnetic este un domeniu contestat în războiul asimetric, în care ambele părți concurează pentru control pentru a obține un avantaj operațional. Congestia spectrului, interferențele de la dispozitivele civile și proliferarea tehnologiilor fără fir complică și mai mult gestionarea spectrului, necesitând capabilități sofisticate de război electronic pentru a funcționa eficient în medii aglomerate și contestate.

Contramăsurile electronice sunt un aspect vital al EW în războiul asimetric. Acestea implică acțiuni întreprinse pentru a proteja forțele prietene de amenințările electronice ale inamicului. În conflictele asimetrice, actorii nestatali sau adversarii mai puțin avansați se bazează adesea pe tactici de gherilă, ascunzându-se în medii urbane sau zone îndepărtate și folosind echipamente electronice rudimentare.

Suportul electronic implică activități care vizează colectarea, interceptarea și analiza semnalelor electronice. În războiul asimetric, acest lucru poate ajuta la identificarea și localizarea pozițiilor inamice, a canalelor de comunicare și a structurilor de comandă. De exemplu, vehiculele aeriene fără pilot (UAV) echipate cu senzori electronici avansați pot oferi informații de neprețuit asupra mișcărilor insurgenților, ajutând la lovituri de precizie sau la operațiuni țintite. Capacitatea de a colecta inteligență electronică este un instrument puternic care poate atenua dezavantajele operațiunii în medii nefamiliare și complexe.

Atacul electronic implică utilizarea energiei electromagnetice pentru a deteriora, perturba sau distruge sistemele electronice ale adversarului. În războiul asimetric, militarii avansați pot folosi atacuri electronice pentru a degrada capacitatea inamicului de a-și coordona, comunica și controla forțele. Acest lucru poate implica utilizarea platformelor de război electronic sau a operațiunilor cibernetice pentru a viza infrastructura de comandă și control a adversarului, perturbând astfel capacitatea acestora de a organiza operațiuni eficiente.

Tendințe emergente în războiul electronic

Principalele tendințe desprinse din studiile de specialitate[2]:

- *Congestia spectrului*: proliferarea tehnologiilor wireless și a dispozitivelor IoT a dus la creșterea congestiei spectrului, ceea ce face mai dificilă operarea în spectrul EM.
- *AI și învățarea automată*: Adversarii încorporează inteligența artificială și învățarea automată în tacticile EW, permițând atacuri electronice mai dinamice și adaptabile.
- *Preocupări juridice și etice*: Utilizarea tehnicilor EW în spațiul cibernetic ridică întrebări juridice și etice, în special în ceea ce privește protecția infrastructurii civile.

În viitorul apropiat, războiul va fi caracterizat de amenințări avansate și inteligente care operează în EMS. Astfel, planificatorii operaționali trebuie să ia în considerare compoziția și

[2] Sfetcu, "Războiul electronic și inteligența artificială."

echilibrul de forțe, iar măsurile EW vor deveni o necesitate pentru sistemele de informare și comunicații în operațiunile militare[3].

Pentru a aborda provocările generate de războiul asimetric, organizațiile militare adoptă câteva tendințe emergente în războiul electronic:

- *EW cognitiv*: Războiul electronic cognitiv (CEW) integrează inteligența artificială (AI) și algoritmii de învățare automată (ML) în sistemele de război electronic pentru a îmbunătăți conștientizarea situației, luarea deciziilor și capacitățile de răspuns. CEW permite analiza în timp real a unor cantități mari de date ale senzorilor, facilitând adaptarea rapidă la amenințările în evoluție și mediile dinamice.
- *EW distribuit*: Războiul electronic distribuit (DEW) descentralizează capabilitățile de război electronic pe mai multe platforme, inclusiv avioane, nave și vehicule terestre, pentru a îmbunătăți supraviețuirea și rezistența împotriva atacurilor inamice. DEW folosește senzori și efectori în rețea pentru a crea un mediu de război electronic distribuit, care să permită operațiuni de colaborare și răspunsuri coordonate la acțiunile adverse.
- *Convergența cibernetică-electronică*: Convergența capacităților de război cibernetic și electronic estompează granițele dintre domeniile fizic și digital, creând sinergii care îmbunătățesc operațiunile ofensive și defensive. *Războiul cibernetic electronic* (CEW) integrează efectele cibernetice, cum ar fi exploatarea rețelei și implementarea programelor malware, cu tehnici tradiționale de război electronic pentru a perturba, degrada sau interzice comunicațiile adversare și sistemele de comandă și control.
- *Contramăsuri adaptive*: Adversarii asimetrici folosesc tactici agile și adaptive pentru a evita detectarea și a neutraliza sistemele de război electronic. Ca răspuns, forțele militare dezvoltă contramăsuri avansate, inclusiv saltul de frecvență, agilitatea formei de undă și sinteza formei de undă, pentru a contracara acțiunile adverse și a menține superioritatea operațională în medii electromagnetice contestate.

Sistemele de război electronic, metodă foarte eficientă de a câștiga victorii importante sau de a obține succese operaționale, nu a primit multă vreme suficientă atenție. Odată cu schimbarea naturii securității, importanța sistemelor de război electronic a reapărut, în special în situații de conflict instabile, iar statele au depus eforturi pentru a face progrese rapide în acest domeniu, pentru avantaje în zonele de conflict din ultimii ani. Ne aflăm deja în perioada de război de a patra generație și amenințările nu sunt aduse doar de echipamente militare feroce, statele folosesc, în

[3] Duke, "Harnessing Chaos."

special, război hibrid și tactici de război asimetrice pentru a crea presiune asupra adversarilor. Sistemele de război electronic sunt intens utilizate în războiul hibrid și asimetric, devenind unul dintre punctele cheie ale viitorilor parametri de securitate. Țările în curs de dezvoltare în special, cu dorința de a deveni o putere regională, pun un accent special pe războiul electronic. Sistemele de război electronic nu mai pot fi ignorate pentru a asigura securitatea și victoria în viitoarelșe războaie sau zone de conflict.

Apariția AI, calculul cuantic, LAWS, armele hipersonice și sistemele DE necesită soluții noi și adesea asimetrice în EMS.

Concluzie

Războiul electronic a evoluat semnificativ de la începuturi, devenind o parte integrantă a operațiunilor militare moderne. Pentru a menține un avantaj competitiv, forțele militare trebuie să se adapteze și să inoveze continuu în acest domeniu. Pe măsură ce tehnologia continuă să avanseze, peisajul războiului electronic va rămâne dinamic, iar provocările emergente vor necesita o abordare cuprinzătoare și cu mai multe fațete. Cercetarea și dezvoltarea continuă în domeniul războiului electronic sunt esențiale pentru a asigura securitatea națională și eficacitatea militară într-o lume din ce în ce mai interconectată și contestată.

Războiul asimetric prezintă provocări și oportunități unice în domeniul războiului electronic, necesitând strategii și tehnologii inovatoare pentru a depăși tacticile de adaptare ale adversarilor și constrângerile de resurse. Prin luarea în considerare a tendințelor emergente, cum ar fi EW cognitiv, EW distribuit, convergența ciber-electronică și contramăsurile adaptive, organizațiile militare își pot îmbunătăți capacitățile de război electronic și își pot menține superioritatea în medii operaționale complexe și dinamice. Navigarea eficientă în peisajul

războiului electronic în scenarii de război asimetric necesită o abordare holistică care să integreze inovația tehnologică cu agilitate strategică și flexibilitate operațională.

Utilizarea războiului electronic în conflicte asimetrice ridică preocupări etice. Potențialul de daune colaterale, încălcarea vieții private și estomparea liniilor dintre combatanți și necombatanți sunt toate dileme etice asociate cu EW. Găsirea echilibrului corect între atingerea obiectivelor militare și respectarea drepturilor omului și a dreptului internațional este o provocare complexă în domeniul războiului electronic.

Războiul electronic este o componentă indispensabilă a războiului asimetric modern. El influențează semnificativ tacticile și strategiile folosite de ambele armate avansate din punct de vedere tehnologic

Bibliografie

Duke, Audrey. “Harnessing Chaos: Unleashing Electromagnetic Warfare for Enhanced Joint Operations,” 2023. https://apps.dtic.mil/sti/citations/AD1206172.

Sfetcu, Nicolae. “Războiul electronic și inteligența artificială.” MultiMedia, January 8, 2024. https://www.telework.ro/ro/e-books/razboiul-electronic-si-inteligenta-artificiala/.